CLAIMS

What is claimed is:

1. A method of providing authentication services for applications that are running on a client and requiring access to a network based server, the method comprising:

establishing a network connection further comprising an authentication with the network;

obtaining, responsive to the authentication, a dynamic seed;

generating an application key corresponding to the dynamic seed; and

providing the application key to facilitate authenticating an application.

2. The method of claim 1 wherein the generating an application key further comprises storing the application key for subsequent retrieval to facilitate the authenticating an application.

3. The method of claim 1 wherein the generating an application key further comprises generating a plurality of application keys where each of the plurality of keys corresponds to a different application.

4. The method of claim 1 wherein the providing the application key further comprises; providing an application seed and generating keying information specific to the application.

5. The method of claim 1 wherein the providing the application key further comprises providing a new application key every time the authenticating the application is required.

6. The method of claim 1 wherein the providing the application key further comprises providing the application key corresponding to a time duration within which the application key is valid.

7. The method of claim 1 wherein the obtaining the dynamic seed further comprises obtaining a new dynamic seed each time an authentication with the network occurs, the generating the application key further comprises generating a new application key corresponding to the new dynamic seed, and the providing the application key further comprises providing the new application key.

8. The method of claim 1 wherein the authentication with the network utilizes processes corresponding to an Extensible Authentication Protocol.

9. The method of claim 1 implemented by one of a client and a network server.

10. The method of claim 9 implemented by one of a wireless client and a network server accessed via a wireless network.

11. A system entity operable to provide authentication services for applications that are running on a client and requiring access to a network based server, the system entity comprising:

a network access function operable to establish a network connection and complete an authentication with the network, the authentication providing a dynamic seed;

a key manager operable to generate an application key that is derived from the dynamic seed; and provide, on demand, the application key to facilitate authenticating an application.

12. The system entity of claim 11 wherein the key manager further stores the application key in persistent storage for subsequent retrieval to facilitate the authenticating an application.

13. The system entity of claim 11 wherein the key manager further generate a plurality of application keys where each of the plurality of keys is derived from the dynamic seed and corresponds to a different application.

14. The system entity of claim 11 wherein the key manager in the providing the application key further provides an application seed; and wherein the system entity further comprises an application entity that is operable to use the application seed for generating keying information specific to the application.

15. The system entity of claim 11 wherein the key manager provides a different application key every time the authenticating the application is required.

16. The system entity of claim 11 wherein the key manager provides the application key and the application key further corresponds to a time duration within which the application key is valid.

17. The system entity of claim 11 wherein the network access function provides a new dynamic seed each time an authentication with the network occurs, and the key manager generates a new application key corresponding to the new dynamic seed and provides the new application key to facilitate the authenticating the application.

18. The system entity of claim 11 wherein the network access function in completing the authentication with the network utilizes processes corresponding to one of a smart card, an Extensible Authentication Protocol with Subscriber Identity Module extensions, an Extensible Authentication Protocol with Transport Level Security extensions, and an Extensible Authentication Protocol with Authentication and Key Agreement extensions.

19. The system entity of claim 11 implemented by one of a client and a network server.

20. The system entity of claim 19 implemented by one of a client operating within a wireless communication unit and a network server accessed via a wireless network.